AO 93 (Rev. 12/09) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

District of New Mexico

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* A Black and Blue Samsung Cellular Phone Bearing IMSI #A0000048AB3C22 (Subject Telehpone #1)	)	Case No. 16-139 MR

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the _____ District of New Mexico
(identify the person or describe the property to be searched and give its location):

Subject Telehpone #1, more fully described in Attachment A, which is attached and fully incorporated herein.

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*:

See Attachment B, which is attached and fully incorporated herein.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before March 1, 2016
(not to exceed 14 days)

☑ in the daytime 6:00 a.m. to 10 p.m. ☐ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge Gregory B. Wormuth .
(name)

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)* ☐ for _____ days *(not to exceed 30)*.

☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 18 Feb 2016 1410 hrs

Judge's signature

City and state: Las Cruces, New Mexico

Gregory B. Wormuth, United States Magistrate Judge
Printed name and title

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
	2/24/16 / 1400	

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

See Attachments Attached

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: 2/24/16

Executing officer's signature

Paul Lujan

Printed name and title

ATTACHMENT A

PROPERTY TO BE SEARCHED

The affidavit, *see* **Attachment C**, is submitted in support of warrants to search and seize information, more fully described in **Attachment B**, contained in the following electronic devices (referred to in **Attachment B** and **Attachment C** as Subject Telephone #1, Subject Telephone #2, and Subject Telephone #3):

Subject Telephone #1

Subject Telephone #1 is described as a black and blue Samsung Verizon, flip-style cellular phone bearing IMSI #A0000048AB3C22. Subject Telephone #1 was seized from Daniel Aran at the time of the execution of a search warrant and Aran's arrest on January 28, 2016. Subject Telephone #1 is currently in the custody of the New Mexico State Police in Las Cruces, New Mexico.

Subject Telephone #2

Subject Telephone #2 is described as a black Verizon Galaxy Note 4, "smart" cellular telephone bearing IMSI #353756073408205. Subject Telephone #2 was seized from Daniel Aran at the time of the execution of a search warrant and Aran's arrest on January 28, 2016. Subject Telephone #2 is currently in the custody of the New Mexico State Police in Las Cruces, New Mexico.

Subject Telephone #3

Subject Telephone #3 is described as a black and blue Samsung Verizon, flip-style cellular telephone bearing IMSI #A0000048D09DD7. Subject Telephone #3 was seized from Daniel Aran at the time of the execution of a search warrant and Aran's arrest on January 28, 2016. Subject Telephone #3 is currently in the custody of the New Mexico State Police in Las Cruces, New Mexico.

ATTACHMENT B

PARTICULAR THINGS TO BE SEIZED/INFORMATION TO BE RETRIEVED

The particular things to be seized include all records, in whatever format, stored on Subject Telephone #1, Subject Telephone #2, and Subject Telephone #3. (collectively referred to as the "Subject Telephones") described in **Attachment A** that are related to violations of 21 U.S.C. §§ 841, including:

1. Digital, cellular, direct connect, and/or other phone numbers, names, addresses, and other identifying information of customers, distributors, sources of supply and other associates of the user of the Subject Telephones;

2. Digital, cellular, direct connect, and/or other phone numbers dialed from, which contacted, or which are otherwise stored on, the Subject Telephones, along with the date and time each such communication occurred;

3. Text message logs and text messages whether sent from, to, or drafted on, the Subject Telephones, along with the date and time each such communication occurred;

4. The content of voice mail messages stored on the Subject Telephones, along with the date and time each such communication occurred;

5. Photographs or video recordings;

6. Information relating to the schedule, whereabouts, or travel of the user of the Subject Telephones;

7. Information relating to other methods of communications utilized by the user of the Subject Telephone's and stored on the Subject Telephones

8. Bank records, checks, credit card bills, account information and other financial records; and

9. Evidence of user attribution showing who used or owned the Subject Telephones, such as logs, phonebooks, saved usernames and passwords, documents, and internet browsing history.

Digital Evidence Unit

T.N.T. - Las Cruces Police Department | Homeland Security Investigations (DHS)
Department: 217 E. Picacho Ave. | Las Cruces NM 88001
Lab: Runnels Federal Building 200 E. Griggs | Las Cruces NM 88001
Phone: (575)528-4200

Case#DEU16018
Suspect:Daniel Aran

DEU Case #: DEU160018
Agency Case#: RBI245D-AQ-5530971
Suspect/Victim: Daniel Aran

Requesting Party:

Agency: LCPD GTF – FBI TFO
Name: P. Lujan

Synopsis:
Three cell phones extraction with Federal Search Warrant.

Submitted Evidence Items Relative to this Report

Cell Phone		Item#19
	Make:	Samsung
	Model:	SM-B311VZPP
	IMEI:	A0000048AB3C22
	Notes:	Phone in evidence bag marked Item #19

Cell Phone		Item#20
	Make:	Samsung
	Model:	SM-B311VZPP
	IMEI:	A0000048D09DD7
	Notes:	Phone in evidence bag marked Item #19

Cell Phone		Item#17
	Make:	Samsung
	Model:	N-910V
	IMEI:	
	Notes:	In a red phone case

NOTE:

All efforts are made to include all pertinent items in generated reports and analysis. Due to manpower and time constraints the information provided is not intended to exclude possible items not documented in Summaries or Reports. Summaries are also not exclusionary and only highlight key items found during the examination of the submitted items. It is necessary to review the generated report media for a full view of digital forensic exam.

Forensic Evaluation Summary

Item 19:

Samsung phone was off in evidence bag. Phone was connected to Cellebrite UFED Touch device and on-screen prompts were followed. Physical Extraction of device was selected and completed. Phone

was loaded into Cellebrite Physical Analyzer (PA). PA processed phone and recovered SMS, Call Logs and Contacts. Another Python script was manually run on device to extract possible deleted text messages (SMS). Script was created by this Investigator. Several messages (deleted) were located on the device. This is not a complete list of deleted messages. Many messages could have been overwritten and are not recoverable. A UFED reader report was generated using the PA program. Refer to instruction sheet for UFED reader application. A second "HTML" webpage based report was also generated. Refer to report media.

Item 20:

Samsung phone was off in evidence bag. Phone was connected to Cellebrite UFED Touch device and on-screen prompts were followed. Physical Extraction of device was selected and completed. Phone was loaded into Cellebrite Physical Analyzer (PA). PA processed phone and recovered SMS, Call Logs and Contacts. Another Python script was manually run on device to extract possible deleted text messages (SMS). Script was created by this Investigator. It appeared that the phone did not have any recoverable deleted messages. This is probably due to the messages not being deleted manually. A UFED reader report was generated using the PA program. Refer to instruction sheet for UFED reader application. A second "HTML" webpage based report was also generated. Refer to report media.

Item 17:

Samsung phone (Note 4) was off in evidence bag. Phone was left off, cable 133 of the Cellebrite UFED 4PC device was used to connect to the phone in a bootloader mode. A physical extraction of the device was completed. Device was then connected to the UFED Touch and a logical extraction of the device was created following on screen instructions.
Cellebrite Physical Analyzer (PA) was used to load the devices resulting extractions. Numerous artifacts were found on the device. PA was used to generate a UFED Reader report as well as an HTML report. Refer to report media.

Generated Reports

RM16019-1:

DVD disc containing 2 extractions of Item 17 (Samsung Note 4). One extraction is a Logical[i] Extraction[ii] and the other is a Physical Extraction. Both are provided for comparison. Both reports are generated in a UFED Reader format that can only be viewed with the UFED Reader application (UFEDReader.exe) found on the media. Refer to UFED Reader overview instructions for more information.

RM16019-2:

CD disc containing the 2 extractions , Item 19 and Item 20. Both reports generated with UFED Reader and can only be viewed using UFED Reader application. Included on the RM is also an HTML webpage report. This report can be opened by opening the Report.html file.

---

[i] *"logical download"*

Data extraction using the device operating system. The tool uses the operating system on the device to retrieve information contained within the phone memory. This method is the quickest method, however the

type of data is usually only that which is live. Deleted data is not typically recovered. It is also limited to SMS, call logs, phone details, phonebook , MMS, images, videos, audio files, and calendar entries.

[ii] *"physical download"*

Data extraction that makes a bit-by-bit copy of the entire memory of a mobile device. This method obtains all data on the device to include the system files. It is the most thorough and can retrieve deleted data. This method requires the tool to have direct access to the memory of the device, and as such is not available on all devices.

Samsung Gusto 3 (SM-B311VZPP) Carving SMS

Text Messages:

Offset	Length	Description
0	1	Message number
3	2	Message data size
119	See (Message data Size)	Text Message in ASCII
160+ Message Length	4	Date (4 byte) Epoch 1/1/1980
207+ Message Length	10	Phone Number (ASCII)
369+ Message Length	1	Message Status x05 – Read, x08 – Unsent(draft) , x00 – Sent ?

?	x00	x00	?	X00	X00	?	?	?	?	X00	X00	X00	X00	?	?
X00	X02	X00	X01	X00	X02	X10	X00	X00	X00	X00	X00	X00	X00	X01	X01
00	00	00	?	?	00	00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	?x0A	0A	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00	?	?	?	?	?	?
?	?	?	?	*	*	*	*	*	*	*	*	*	*	*	*
*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
*	*	*	*	*	*	*	*	*	*	*	*				

GREP expression:

'.{1}\x00{2}.{1}\x00{2}.{4}\x00{4}.{2}\x00\x02\x00\x01\x00\x02\x10\x00{7}\x01\x01\x00{3}.{2}\x00{82}.+?(?=\x0A)\x0A{1}\x00{19}.{10}.{185}'

6862/29/2016